VA outlines data security upgrades

05/25/06 -- 05:03 PM, *By Mary Mosquera,*

The Veterans Affairs Department is tightening its data security policies in response to the theft of sensitive, private electronic data of 26.5 million veterans.

At the same time, VA officials are trying to notify and equip veterans with the means to determine whether their identities may have been compromised or stolen, VA Secretary Jim Nicholson told lawmakers today.

Nicholson disclosed that it took two weeks after the theft for him to be alerted by VA officials.

“I’m outraged at the loss of veterans’ personal data. I’m frankly mad as hell. I am gravely concerned about the timing of the department’s response once the burglary became known,” he told the House Veterans Affairs Committee.

VA will publish upgraded data security guidelines for single-user remote access in a directive by June 30, he said.

“I can promise you that we will do everything in our power to make clear what is appropriate and inappropriate use of data by our employees,” Nicholson told lawmakers during testimony before both the House and Senate veterans’ committees.

VA has begun discussions regarding the immediate automatic encryption of all sensitive information.

Other changes that the department is implementing to centralize IT management and budget authority under the VA CIO will also strengthen compliance and enforcement of data privacy and security policies, other VA officials said.

Nicholson announced that President Bush yesterday nominated Robert Howard to be acting CIO and acting assistant secretary for information and technology. Howard has been supervising the CIO’s office since May 1 after former CIO Robert McFarland left VA.

A VA data analyst reported May 3 the theft of his laptop, disks and coins from his home in the Aspen Hill area of Montgomery County, Md. Nicholson publicly announced what lawmakers called the largest breach ever of Social Security numbers earlier this week.

According to law enforcement officials, VA data did not appear to be the target of the theft, and the data does not appear to have been compromised.

The analyst, who is on administrative leave, had authority to access the sensitive data but violated VA policy by taking the data outside the department, Nicholson said. The data was not encrypted. The employee was working on simplifying some data processes for a national veterans’ survey.

VA inspector general George Opfer said he would complete in 45 days an administrative investigation into the department’s security and privacy policies and procedures, the length of time to notify officials through the chain of command and the recommendations. He will also conduct a criminal investigation to be delivered later.

VA will conduct an inventory of those with access to sensitive VA data and review their positions requiring access to that data. Those employees will undergo an updated background check or ask the FBI for background investigations depending on the level of access and responsibilities.

VA will accelerate the requirement that all employees complete a cybersecurity training course by June 30. This course includes learning provisions of the Privacy Act, what is unauthorized disclosure or use of sensitive information in the course of employment at VA, and details of loss or unauthorized use of federal property and its repercussions. VA employees must sign an annual statement of their awareness of privacy and security responsibilities and consequences of disclosing personal information.

As a result of the theft, VA may have to spend up to $250 million to pay for credit reports, monitoring and potential damage that results from the theft, according to Nicholson.

VA would have to get authority and funding to pay for actions beyond paying for credit reports.
http://www.gcn.com/online/vol1_no1/40862-1.html